

Blind quantum computation with noise environment

Yu-Bo Sheng,^{1*} Lan Zhou²

¹*Key Lab of Broadband Wireless Communication and Sensor Network Technology,
Nanjing University of Posts and Telecommunications,
Ministry of Education, Nanjing, 210003, China*

²*College of Mathematics & Physics,
Nanjing University of Posts and Telecommunications,
Nanjing, 210003, China*

(Dated: September 29, 2016)

Blind quantum computation (BQC) is a new type of quantum computation model. BQC allows a client (Alice) who does not have enough sophisticated technology and knowledge to perform universal quantum computation and resorts a remote quantum computation server (Bob) to delegate universal quantum computation. During the computation, Bob cannot know Alice's inputs, algorithm and outputs. In single-server BQC protocol, it requires Alice to prepare and distribute single-photon states to Bob. Unfortunately, the distributed single photons will suffer from noise, which not only makes the single-photon state decoherence, but also makes it loss. In this protocol, we describe an anti-noise BQC protocol, which combined the ideas of faithful distribution of single-photon state in collective noise, the feasible quantum nondemolition measurement and Broadbent-Fitzsimons-Kashefi (BFK) protocol. This protocol has several advantages. First, Alice does not require any auxiliary resources, which reduces the client's economic cost. Second, this protocol not only can protect the state from the collective noise, but also can distill the single photon from photon loss. Third, the noise setup in Bob is based on the linear optics, and it is also feasible in experiment. This anti-noise BQC may show that it is possible to perform the BQC protocol in a noisy environment.

PACS numbers: 03.67.Ac, 03.65.Ud, 03.67.Lx

I. INTRODUCTION

Quantum computation has attracted much interest for its ultrafast computation ability. Shor's algorithm for integer factorization [1], Grover's algorithm and the optimal Long's algorithm for unsorted database search [2, 3], all have displayed the great computing power of quantum computers. Small-scale quantum computers in ions [4], superconduction [5], photons [6], and some other important quantum systems have been widely investigated [7]. It is not a dream to successfully product a quantum computer in the foreseeable future. Like current supercomputers, the first generation of quantum computers must be very expensive and owned by very few governments or big companies. As an ordinary quantum computer client, he or she has poor quantum ability and are insufficient to realize universal quantum computation. Certainly, he or she can resort the quantum computation server's help to realize the computation. Moreover, he or she should protect his data without leakage. Blind quantum computation (BQC) is a new type of quantum computation model that the client who does not have enough quantum knowledge and sophisticated technology and resorts the quantum computation servers to perform the universal quantum computation. During the computation, the client's inputs, algorithms and outputs should be absolutely security.

In 2005, Childs proposed the first BQC model [8]. It is the standard quantum circuit model. Bob needs to perform the quantum gates and Alice requires the quantum memory. In 2009, Broadbent, Fitzsimons, and Kashefi (BFK) proposed a BQC protocol based on the one-way quantum computation model [9]. In their protocol, Alice only requires to generate the single-qubit quantum state and a classical computer. The most advantage of this protocol is that Alice does not need the quantum memory. There are also some other important BQC protocols [10–28]. For example, Morimae *et al.* proposed two BQC protocols based on the Affleck-Kennedy-Lieb-Tasaki state [10]. Fitzsimons and Kashefi constructed a new verifiable BQC protocol [12]. The experiment of the BFK protocol based on the optical system was also reported [17]. Generally, these kinds of BQC protocols can be divided into three groups. The first group is the single-server BQC model [8–10, 12–17, 19–25, 28]. The second group is double-server BQC model [9, 18, 27] and the third group is triple-server BQC model [26]. In single-server BQC model, the client Alice is required to has the quantum ability of generating and distributing the single quantum states. In double-server BQC model and triple-server BQC model, the client Alice can be completely classical.

In single-server BQC protocol, the client Alice should distribute the single-photon states to the server Bob. In previous single-server protocols, the quantum channel is assumed to be ideal. However, the ideal quantum channel does not exist, and all the quantum states will suffer from noise. The environment noise will make the

*shengyb@njupt.edu.cn

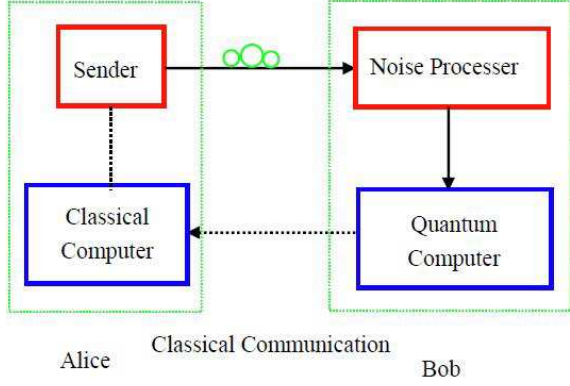


FIG. 1: Schematic of the anti-noise BQC protocol. After Alice prepares and encodes the single-photon state $|+\theta_j\rangle$ to resist the collective noise using the Sender modular. Bob distills the polluted single-photon state using the Noise Processor modular, before starting the BQC protocol.

quantum state become error, and it will also make the distributed photons loss. In quantum communication, various error correction and error rejection methods are proposed [29–34]. For instance, Walton *et al.* proposed a scheme for rejecting the errors introduced by noise with decoherence-free subspaces [29]. In 2005, Kalamidas proposed two interesting linear-optical single photon schemes to reject and correct arbitrary qubit errors without additional particles [30]. By adding one extra photon with a fixed polarization, a distribution scheme of polarization states of a single photon over a collective-noise channel was proposed [31]. In 2007, Li and Deng described a faithful qubit transmission scheme with linear optics against collective noise without ancillary qubits [32]. On the other hand, quantum state amplification is an efficient tools to resist the photon loss [35–42]. The quantum state amplification can increase the probability of single photon and decrease the probability of photon loss.

Practical BQC protocol should also works under the noise environment. In double-server BQC, Morimae and Fujii first described an efficient secure entanglement distillation for double-Server BQC [18]. They showed that it is possible to perform entanglement distillation in the double-server scheme without degrading the security of blind quantum computing. In 2015, we proposed the deterministic entanglement distillation for secure double-server BQC [27]. In single-server BQC, recently, Takeuchi *et al.* first considered the model of single-server BQC over a collective-noise channel, which is called DFS-BQC [28]. They described three variations of DFS-BQC protocols, combined the ideas based on the DFS and the BFK protocol. In this paper, we describe another anti-noise BQC protocol, based on the original BFK protocol [9]. This protocol has some advantages.

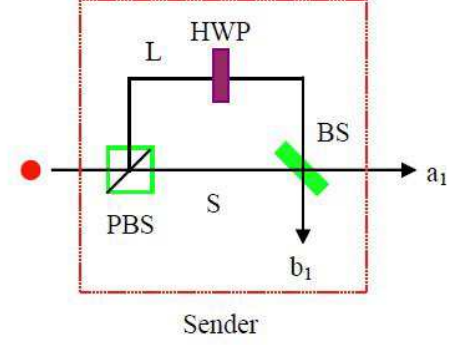


FIG. 2: Schematic of the Sender modular as shown in Fig. 1. BS is the 50:50 beam splitter and PBS is the polarization beam splitter. HWP is the half-wave plate which can convert $|H\rangle$ polarization photon to $|V\rangle$ polarization photon and vice versa. L and S are the long and short arm of the photon.

First, Alice does not require to generate the Bell pair or coherent light, and only to distribute and operate the single photon with linear optics. which reduces the client's economic cost. Second, this protocol not only can protect the state from the collective noise, but also can distill the single photon from the photon loss. Third, the noise setup in Bob is based on the feasible linear optics.

II. BASIC MODEL OF ANTI-NOISE BQC PROTOCOL

Before we explain this protocol, we first briefly describe the original BFK protocol. It runs as follows [9]: a) Client Alice first prepares n rotated qubits $\{|+\theta_j\rangle \equiv (|0\rangle + e^{i\theta_j}|1\rangle)/\sqrt{2}\}_{j=1}^n$ and distributes to the server Bob. Here $\theta_j \in \{k\pi/4 \mid k \in \mathbb{Z}, 0 \leq k \leq 7\}$ and E is the set of edges of G and $CZ_{i,j}$ is the CZ gate between the i th and j th qubits. b) Bob prepares the Graph state G , which Alice tells her. Here $|G\{\theta_j\}\rangle \equiv (\bigotimes_{i,j \in E} CZ_{i,j})|+\theta_j\rangle$. c) Bob performs the measurement on the j th qubit according to measurement angle $\xi_j = \theta_j + \phi'_j + r_j\pi$, which Alice tells her. Here r_j is a random number and $r_j \in \{0, 1\}$. ϕ'_j is the modified version of ϕ_j according to the previous measurement results. d) Bob sends the measurement results to Alice and Alice completes the computation with classical computer.

The basic model of this anti-noise BQC protocol is shown in Fig. 1. In the side of Alice, Alice first prepare n rotated qubits $\{|+\theta_j\rangle \equiv (|0\rangle + e^{i\theta_j}|1\rangle)/\sqrt{2}\}_{j=1}^n$. In an optical system, we denote the horizontal polarization photon $|H\rangle$ as $|0\rangle$ and vertical polarization photon $|V\rangle$ as $|1\rangle$, respectively. In traditional BFK protocol, the single-photon state $|+\theta_j\rangle$ is sent to Bob directly. In this protocol, Alice first encodes the state $|+\theta_j\rangle$ as shown in Fig. 2.

$$|+\theta_j\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\theta_j}|V\rangle) \rightarrow \frac{1}{\sqrt{2}}(|H_S\rangle + e^{i\theta_j}|H_L\rangle)$$

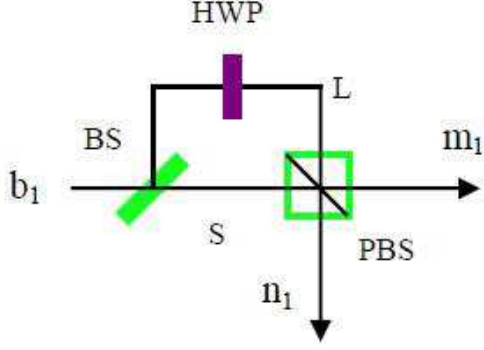


FIG. 4: Schematic of decoding if the single photon is in the spatial mode b_1 .

linear noiseless amplification (NLA) to complete the task. Here we introduce a pair of ancillary polarized photons of the form

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}). \quad (9)$$

As shown in Fig. 3, the partially polarization beam splitter (PPBS₁) can reflect the vertically polarized photon totally, while reflect the horizontally polarized photon with the coefficient of γ , and transmit it with the coefficient of $1 - \gamma$. Another PPBS₂ can transmit the horizontally polarized photon totally, while reflect the vertically polarized photon with the coefficient γ , and transmit it with the coefficient of $1 - \gamma$. For instance, the PPBS₁ can make [39]

$$\begin{aligned} \hat{a}_{c_1,H}^\dagger|0\rangle &\rightarrow \gamma\hat{a}_{out,H}^\dagger|0\rangle + \sqrt{1-\gamma^2}\hat{a}_{D_1,H}^\dagger|0\rangle, \\ \hat{a}_{k_1,H}^\dagger|0\rangle &\rightarrow -\gamma\hat{a}_{D_1,H}^\dagger|0\rangle + \sqrt{1-\gamma^2}\hat{a}_{out,H}^\dagger|0\rangle, \\ \hat{a}_{k_1,V}^\dagger|0\rangle &\rightarrow -\hat{a}_{D_1,V}^\dagger|0\rangle. \end{aligned} \quad (10)$$

Here \hat{a}^\dagger is the creation operator. The subscripts c_1 , out , k_1 and k_2 are the spatial modes as shown in Fig. 3. Therefore, by using PPBS₁ and PPBS₂, we can obtain the relationship

$$\begin{aligned} |0_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{\gamma}{2}|0_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle), \\ |0_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{\gamma}{2}|0_{out}\rangle(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle \\ &\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle), \\ |H_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{(2\gamma^2-1)}{2}|H_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle), \\ |H_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{\gamma^2}{2}|H_{out}\rangle(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle \\ &\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle), \\ |V_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{\gamma^2}{2}|V_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \end{aligned}$$

$$\begin{aligned} &+ |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle), \\ |V_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{(2\gamma^2-1)}{2}|V_{out}\rangle(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle \\ &\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle). \end{aligned} \quad (11)$$

The mixed state ρ'_{θ_j} combined with the polarization Bell state $|\phi_1\rangle$ can be described as follows. With the probability of F , it is in the state $|\varphi\rangle \otimes |\phi_1\rangle$ and with the probability of $1 - F$, it is in the state $|vac\rangle \otimes |\phi_1\rangle$. We first discuss the item $|\varphi\rangle \otimes |\phi_1\rangle$. It evolves as

$$\begin{aligned} |\varphi\rangle \otimes |\phi_1\rangle &= \left[\frac{\alpha}{\sqrt{2}}|+\theta_j\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \right. \\ &+ \frac{\beta}{\sqrt{2}}|0\rangle_{c_1}|+\theta_j\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &+ \frac{\tau}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|+\theta_j\rangle_{m_1}|0\rangle_{n_1} \\ &+ \frac{\delta}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|+\theta_j\rangle_{n_1}] \\ &\otimes \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}). \end{aligned} \quad (12)$$

The first item evolves as

$$\begin{aligned} &\frac{\alpha}{\sqrt{2}}|+\theta_j\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\otimes \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}) \\ &= \frac{\alpha}{2\sqrt{2}}(|H\rangle_{c_1}|H\rangle_{k_1}|H\rangle_{k_2} + |H\rangle_{c_1}|V\rangle_{k_1}|V\rangle_{k_2} \\ &\quad + e^{i\theta}|V\rangle_{c_1}|H\rangle_{k_1}|H\rangle_{k_2} + e^{i\theta}|V\rangle_{c_1}|V\rangle_{k_1}|V\rangle_{k_2}) \\ &\otimes |0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\rightarrow \frac{\alpha}{2\sqrt{2}}\left[\frac{(2\gamma^2-1)}{2}|H_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \right. \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\quad + \frac{\gamma^2}{2}|V_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\quad + e^{i\theta}\frac{\gamma^2}{2}|V_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\quad + \frac{(2\gamma^2-1)}{2}|V_{out}\rangle(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle \\ &\quad \left. - e^{i\theta}|V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\right]. \end{aligned} \quad (13)$$

The second item can evolve as

$$\begin{aligned} &\frac{\beta}{\sqrt{2}}|0\rangle_{c_1}|+\theta_j\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\ &\otimes \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}) \\ &\rightarrow \frac{\beta\gamma}{4}(|0_{out}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle \\ &\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle) \end{aligned}$$

$$\begin{aligned}
& + |0_{out}\rangle(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle) \\
& \otimes |+\rangle_{\theta_j}|0\rangle_{m_1}|0\rangle_{n_1} \\
& = \frac{\beta\gamma}{4}|0_{out}\rangle|+\rangle_{\theta_j}|0\rangle_{m_1}|0\rangle_{n_1}(|H_{D_1}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle).
\end{aligned}
\tag{14}$$

The third item can evolve as

$$\begin{aligned}
& \frac{\tau}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|+\rangle_{\theta_j}|0\rangle_{n_1} \\
& \otimes \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}) \\
& \rightarrow \frac{\tau\gamma}{4}|0\rangle_{c_1}|0\rangle_{d_1}|+\rangle_{\theta_j}|0\rangle_{n_1}(|H_{D_1}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle).
\end{aligned}
\tag{15}$$

The forth item can evolve as

$$\begin{aligned}
& \frac{\delta}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|+\rangle_{\theta_j}|0\rangle_{n_1} \\
& \otimes \frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}) \\
& \rightarrow \frac{\delta\gamma}{4}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|+\rangle_{\theta_j}|0\rangle_{n_1}(|H_{D_1}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle).
\end{aligned}
\tag{16}$$

Interestingly, from Eq. (13) to (16), if they pick up the case that the single-photon detectors D_1D_4 or D_2D_3 register one photon respectively, they will obtain the state $|+\rangle_{\theta_j}$ deterministically in the output mode, for the cases in Eq. (14) to (16) can not lead both single-photon detectors D_1D_4 or D_2D_3 register one photon, and only the item in Eq. (13) can satisfy the selection condition.

Once Bob obtain the single-photon state $|+\rangle_{\theta_j}$ deterministically, he can start to perform the BQC protocol. In this way, the whole BQC protocol can be modified as follows: 1) Alice prepares n rotated qubits $\{|+\rangle_{\theta_j}\}_{j=1}^n$. 2) Alice encodes the photon $|+\rangle_{\theta_j}$ with linear optics, as shown in Fig. 2. 3) Alice distributes the photon to Bob, which will suffer from collective noise and photon loss. 4) Bob distill the polluted single-photon states with Noise Processer setup, as shown in Fig. 3. 5) Bob prepares the Graph state G . 6) Bob performs the measurement on the j th qubit. 7) Bob sends the measurement results to Alice and Alice completes the computation with classical computer.

III. DISCUSSION AND CONCLUSION

So far, we have completely explained the anti-noise BQC protocol. In original BQC protocol, Alice prepares and distributes the state $|+\rangle_{\theta_j}$ directly. Bob also receives the $|+\rangle_{\theta_j}$ and perform the BQC subsequently, for they do not consider the noise environment. Similar to the pioneer work of Ref.[28] in collective-noise BQC protocol, Alice and Bob should perform the pretreatment for noise, before starting the BQC protocol, following the

approaches suggested in Refs.[32, 39]. In BQC protocol, two essential properties are correctness and blindness. The correctness means that the output of the protocol in Alice's desired one as long as Alice and Bob follow the procedure of the protocol is faithfully. On the other hand, the blindness means that Bob cannot know any information about Alice's inputs, algorithm, and outputs, whenever Alice follows the procedure of the protocol. Obviously, this protocol is correctness for Bob can obtain the faithful qubits after the Noise Processer. On the other hand, this protocol is also blindness. The information sent from Alice to Bob is $|+\rangle_{\theta_j}$, which is decided by θ_j . Bob does not know the exact information of θ_j , which ensures that the protocol is blindness.

We can calculate the total success probability of this protocol. From Fig. 2, we explain this protocol by selecting the case that the photon being in the spatial mode a_1 with the probability of 50%. Actually, if the photon is in the spatial mode b_1 , they can perform the protocol with the same principle. That is to say, if the photon does not lose and only suffer from the collective noise, by picking up the suitable arriving time $SL(LS)$ as shown in Fig. 4, the total success probability is 50%. On the other hand, as shown in Fig. 3, such setup essentially distill the photons in the spatial modes c_1 , i. e., the first item in Eq. (7). Actually, in Eq. (7), other three items which contains the single photon that can also be verified by adding three auxiliary polarized Bell states. The final success probability of this protocol can be calculated as

$$P = \frac{F(5\gamma^4 - 4\gamma^2 + 1)}{32}. \tag{17}$$

In the previous work of Ref.[28], they presented three important BQC protocols over a collective-noise channel. The first protocol is entanglement-based protocol. The second is single-photon-based protocol and the third is the coherent-light-assisted protocol. The common characteristics of three protocol is that they require auxiliary resources, such as entanglement, single photon or coherent light. Moreover, these protocols suppose that Bob has powerful QND measurement, which can distinguish the arriving photons deterministically. However, they do not explain how to realize such QND measurement. In current technology, QND measurement, such as exploiting cross-Kerr nonlinearity has widely discussed in quantum information processing [43–47], but it is still a big challenge in experiment [48] and it will greatly increase the computation cost.

In conclusion, we have described an efficient anti-noise BQC protocol. Different from previous work, this protocol has several advantages. First, this protocol does not require any auxiliary resources, which makes the client is economic. Second, this protocol not only can protect the state from the collective noise, but also from the photon loss. Third, the Noise Processer for Bob is based on the linear optics, and it is also feasible in experiment.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China under Grant Nos. 11474168

and 61401222, the Qing Lan Project in Jiangsu Province, and a Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions.

-
- [1] P. W. Shor, Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE, 124-134 (1994).
 - [2] L. K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 212-219 (1996).
 - [3] G. L. Long, Phys. Rev. A **64**, 022307 (2001).
 - [4] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
 - [5] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001).
 - [6] C.-Y. Lu, *et al.*, Nat. Phys. **3**, 91 (2007).
 - [7] J. Berezovsky, M. H. Mikkelsen, N. G. Stoltz, L. A. Coldren, and D. D. Awschalom, Science **320**, 349 (2008); R. Hanson and D. D. Awschalom, Nature **453**, 1043 (2008).
 - [8] A. Childs, Quantum Inf. Comput. **5**, 456 (2005).
 - [9] A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, Piscataway, NJ, 2009), p. 517.
 - [10] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486.
 - [11] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
 - [12] J. Fitzsimons, and E. Kashefi, arXiv:1203.5217.
 - [13] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
 - [14] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
 - [15] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
 - [16] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).
 - [17] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
 - [18] T. Morimae and K. Fujii, Phys. Rev. Lett. **111**, 020502 (2013).
 - [19] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).
 - [20] A. Mantri, C. A. P. Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).
 - [21] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).
 - [22] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
 - [23] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Nat. Commun. **5**, 3074 (2014).
 - [24] T. Morimae, Phys. Rev. A **89**, 060302(R) (2014).
 - [25] A. Gheorghiu, E. Kashefi, and P. Wallden, New J. Phys. **17**, 083040 (2015).
 - [26] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Phys. Rev. A **89**, 040302(R) (2014).
 - [27] Y. B. Sheng, and L. Zhou, Sci. Rep. **15**, 7815 (2015).
 - [28] V. Takeuchi, K. Fujii, R. Ikuta, T. Yamamoto, and N. Imoto, Phys. Rev. A **93**, 052307 (2016).
 - [29] D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
 - [30] D. Kalamidas, Phys. Lett. A **343**, 331(2005).
 - [31] T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005).
 - [32] X. H. Li, F. G. Deng, and H. Y. Zhou, Appl. Phys. Lett. **91**, 144101 (2007).
 - [33] Y. B. Sheng, and F. G. Deng, Phys. Rev. A **81**, 042332 (2010).
 - [34] H. Kumagai, . Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **87**, 052325 (2013).
 - [35] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
 - [36] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).
 - [37] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R.T. Thew, Phys. Rev. A **86**, 023815 (2012).
 - [38] S. L. Zhang, S. Yang, X.B. Zou, B.S. Shi, and G.C. Guo, Phys. Rev. A **86**, 034302 (2012).
 - [39] E., Meyer-Scott, M., Bula, K. Bartkiewicz, A. Černoč, J. Soubusta, T. Jennewein, and K. Lemr, Phys. Rev. A **88**, 012327 (2013).
 - [40] Y. B. Sheng, Y. Ou-Yang, L. Zhou, and L. Wang, Quantum Inf. Process. **13**, 1595 (2014).
 - [41] Z. F. Feng, Y. Ou-Yang, L. Zhou, and Y.B. Sheng, Opt. Commun. **340**, 80 (2015).
 - [42] N. Bruno, V. Pini, A. Martin, V. B. Verma, S. W. Nam, R. Mirin, A. Lita, F. Marsili, B. Kroz, F. Bussi eres, N. Sangouard, H. Zbinden, N. Gisin, and R. Thew, Opt. Express **24**, 125 (2016).
 - [43] K. Nemoto and W. J. Munro, Phys. Rev. Lett. **93**, 250502 (2004).
 - [44] B. He, Y. Ren, and J. A. Bergou, Phys. Rev. A **79**, 052323 (2009).
 - [45] Y. B. Sheng, and L. Zhou, Sci. Rep. **5**, 13453 (2015).
 - [46] D. Ding, F. L. Yan, and T. Gao, Sci. China-Phys. Mecha. & Astro. **57**, 2098 (2014).
 - [47] L. Dong , J. X. Wang, Q. Y. Li, H. Z. Shen, H. K. Dong, X. M. Xiu, Y. J. Gao, and H. O. Choo, Phys. Rev. A **93**, 012308 (2016).
 - [48] P. Kok, W. J. Munro, K. Nemoto, T. C. Palph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).